549308

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年9 月30 日 (30.09.2004)

PCT

(10) 国際公開番号
WO 2004/084483 A1

(51) 国際特許分類[7]: H04L 9/08, G09C 1/00, G06F 17/30, 17/60, 12/14

(21) 国際出願番号: PCT/JP2003/003413

(22) 国際出願日: 2003 年3 月20 日 (20.03.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 株式会社日本医療データセンター (JAPAN MEDICAL DATA CENTER CO., LTD.) [JP/JP]; 〒102-0083 東京都 千代田区 麹町三丁目 1 番地 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 岡 博志 (OKA,Hiroshi) [JP/JP]; 〒164-0003 東京都 中野区 東中野二丁目１３番４号 Tokyo (JP). 木村 真也 (KIMURA,Shinya) [JP/JP]; 〒651-2275 兵庫県 神戸市西区 樫野台五丁目２番地 C－１４０７ Hyogo (JP).

(74) 代理人: 黒田 健二, 外 (KURODA,Kenji et al.); 〒105-0001 東京都 港区 虎ノ門３丁目６番２号 第２秋山ビル４階・５階 黒田特許事務所 Tokyo (JP).

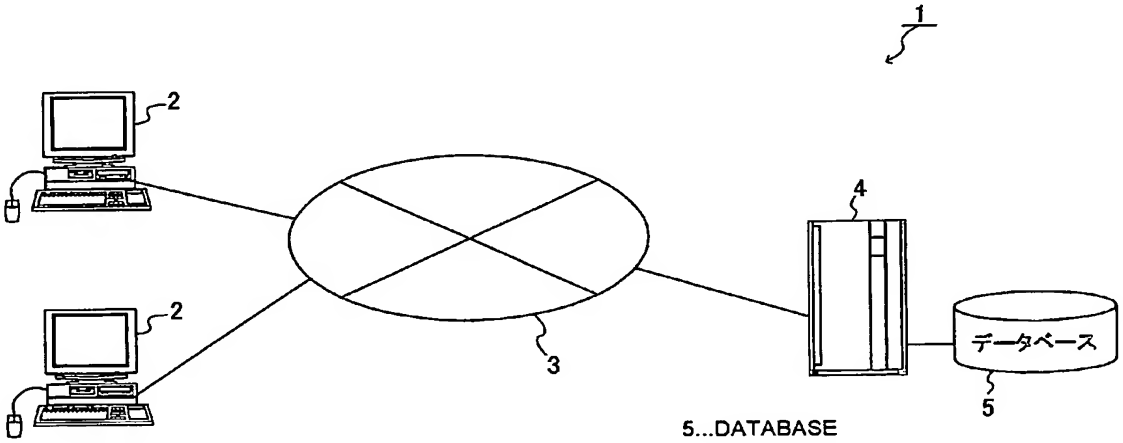
(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM,

[続葉有]

(54) Title: INFORMATION MANAGEMENT SYSTEM

(54) 発明の名称: 情報管理システム



(57) Abstract: An information management system for surely protecting personal information while securing informational availability in processing data including personal information. In an information management system (1), processing target data including the personal information are acquired by an information manager (2), and personal information is extracted from the processing target data and arithmetically operated with a unidirectional function on the basis of the extracted personal information to generate a unique code. The personal information included by the processing target data is substituted with the unique code to generate primary conversion data. This primary conversion data is transmitted from the information manager (2) to an information center unit (4) and stored in a database (5) and used for statistical processing.

(57) 要約: 個人情報を含むデータを処理する際に、情報の有用性を確保しながら個人情報を確実に保護することが可能な情報管理システムを提供する。情報管理システム（１）において、個人情報を含む処理対象のデータを情報管理装置（２）によって取得し、処理対象のデータから個人情報を抽出し、抽出した個人情報をもとに、一方向関数による演算を行ってユニークコードを生成する。そして、処理対象のデータに含まれる個人情報をユニークコードに置き換えることで、一次変換データを生成し、この一次変換データを情報管理装置（２）から情報センタ装置（４）に送信し、データベース（５）に格納して、統計的処理に用いる。

WO 2004/084483 A1

AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明　細　書

情報管理システム

技術分野

本発明は、個人情報を含む情報を管理する情報管理システムに関する。

背景技術

情報化の進展により、政府機関、民間企業、公益団体等においては、電子化された大量の情報が取り扱われるようになった。電子化された情報は、蓄積、検索、複製等の処理を簡単に行うことができ、さらに詳細な分析を行うなどの高度なデータ処理を行えるため、有用性が高い。

ところで、上記電子化された情報は、個人の氏名、生年月日、住所、電話番号、性別、家族構成等の個人情報を含むことが少なくない。個人情報は、悪用やプライバシーの侵害を防止するために慎重に取り扱われなければならず、必要に応じて隠蔽する必要がある。

しかし、例えば個人の属性に関する情報を統計的に処理する場合、個人情報を含む情報を大量に収集せざるを得ないので、厳重に情報管理を行うために多大な労力が費やされる。そこで、個人情報を効率よく確実に保護する方法が、種々検討されていた。

例えば、個人情報を示す文字列を、全て無意味な文字や記号に置き換える方法があった。しかしこの方法では、個人情報が完全に失われてしまうため、例えば、一人の人物に関する複数の情報と、複数の人物に関する複数の情報との見分けがつかなくなってしまうといった問題が生じる。この問題により、統計的処理に際して母集団の数が曖昧となり分析の精度が低下するなど、不都合を生じる恐れがあった。

そこで、個人情報を示す文字列の一部のみに、文字の並べ替えや他の文字への置き換え等の単純な操作を施す方法があった。この方法では、個人情報の一部がもとの状態を保つので、例えば操作後の複数の個人情報を参照して、同一人物に

関する情報か別人に関する情報かを判別することは、一応可能である。しかし、この方法では、操作後の個人情報を分析することで規則性が見いだされ、いかなる操作が行われたのかが判明してしまう可能性があった。このため、個人の健康状態や資産に関する情報等の厳重に管理すべき情報を取り扱う場合には、セキュリティ上の懸念から、上記の方法を使うことはできなかった。

このように、個人情報を隠蔽するために、処理対象の個人情報に操作を施す場合、操作が複雑だと情報の有用性を損なってしまい、操作が単純だと個人情報を確実に保護することができないという問題があった。

そこで、個人情報を含む情報をパスワードを用いて暗号化する方法が採用されていた。しかしこの方法では、パスワードを、消失や漏洩が無いように管理しなければならず、管理負担が大きいという問題があった。また、多くの情報を暗号化して保管し、利用時に復号するといった方法では、情報を暗号化および復号する手間がかかり、情報処理の効率が低くなるという問題があった。

発明の開示

本発明は、個人情報を含む情報を処理する際に、情報の有用性を損なうことなく、個人情報を確実に保護することが可能な情報管理システムを提供することを目的とする。

上記の目的を達成するため、第１の発明は、

個人情報を含むデータを処理する情報管理装置であって、処理対象のデータから個人情報を抽出する個人情報抽出手段と、前記個人情報抽出手段により抽出された個人情報をもとに一方向関数を用いた演算を行ってユニークコードを生成するユニークコード生成手段と、前記処理対象のデータ中の個人情報を前記ユニークコードに置き換えて一次変換データを生成する一次変換データ生成手段とを備えたことを特徴とする。

第２の発明は、第１の発明の情報管理装置において、前記一次変換データと、前記一次変換データのもとになった前記処理対象のデータとを対応づけて記憶する記憶手段をさらに備えることを特徴とする。

第３の発明は、第１の発明の情報管理装置において、前記ユニークコード生成

手段は、前記個人情報抽出手段により抽出された個人情報から基準文字列を生成する基準文字列生成手段と、前記基準文字列をキーとして、所定の演算対象文字列を前記一方向関数により演算することによって、前記ユニークコードを生成する演算手段とを備えて構成されることを特徴とする。

第４の発明は、第３の発明の情報管理装置において、前記演算手段は、前記基準文字列に基づいて演算桁数を決定する桁数決定手段と、前記演算桁数を有する演算対象文字列を生成する演算対象文字列生成手段と、前記基準文字列をキーとして前記演算対象文字列を前記一方向関数により演算する演算実行手段とを備えて構成されることを特徴とする。

第５の発明は、第１の発明の情報管理装置において、前記一次変換データを暗号化して二次変換データを生成する二次変換データ生成手段と、前記二次変換データを他の装置へ出力する出力手段と、前記出力手段により前記二次変換データが出力された際に、出力された前記二次変換データと、前記二次変換データのもとになった前記一次変換データと、前記一次変換データのもとになった前記処理対象のデータと、前記出力手段による出力記録とを対応づけて記憶する記憶手段と、をさらに備えることを特徴とする。

第６の発明は、個人情報を含むデータを処理する情報管理装置と、前記情報管理装置により処理されたデータを管理する情報センタ装置とが通信回線を介して接続されてなる情報管理システムであって、前記情報管理装置は、処理対象のデータから個人情報を抽出する個人情報抽出手段と、前記個人情報抽出手段により抽出された個人情報をもとに一方向関数を用いた演算を行ってユニークコードを生成するユニークコード生成手段と、前記処理対象のデータ中の個人情報を前記ユニークコードに置き換えて一次変換データを生成する一次変換データ生成手段と、前記一次変換データを暗号化して二次変換データを生成する二次変換データ生成手段と、前記二次変換データを、前記通信回線を介して前記情報管理装置に出力する出力手段と、前記出力手段により前記二次変換データが出力された際に、出力された前記二次変換データと、前記二次変換データのもとになった前記一次変換データと、前記一次変換データのもとになった前記処理対象のデータと、前記出力手段による出力の記録とを対応づけて記憶する記憶手段とを備え、前記情

報センタ装置は、前記情報管理装置から送信された二次変換データを受信する受信手段と、前記受信手段により受信された二次変換データを復号して前記一次変換データを生成する復号手段とを備えることを特徴とする。

第７の発明は、第６の発明の情報管理システムにおいて、前記情報センタ装置は、前記復号手段により生成された一次変換データを格納するデータ格納手段をさらに備え、前記データ格納手段に格納されたデータを、前記ユニークコードをキーとして処理することを特徴とする。

第８の発明は、第７の発明の情報管理システムにおいて、前記情報センタ装置は、前記データ格納手段に格納された、前記ユニークコードを含む複数のデータの中から、同一のユニークコードを含むデータを検出することを特徴とする。

第９の発明は、個人情報を含むデータを処理する情報管理用コンピュータに、個人情報抽出手段によって処理対象のデータから個人情報を抽出するステップと、ユニークコード生成手段によって前記個人情報抽出手段により抽出された個人情報をもとに一方向関数を用いた演算を行ってユニークコードを生成するステップと、一次変換データ生成手段によって前記処理対象のデータ中の個人情報を前記ユニークコードに置き換えて一次変換データを生成するステップとを含む処理を実行させるためのプログラムである。

第１０の発明は、第９の発明のプログラムであって、前記情報管理用コンピュータに、前記一次変換データと、前記一次変換データのもとになった前記処理対象のデータとを対応づけて記憶手段に記憶するステップをさらに含む処理を実行させることを特徴とする。

第１１の発明は、第９の発明のプログラムであって、前記ユニークコード生成手段によりユニークコードを生成するステップは、前記個人情報抽出手段により抽出された個人情報から基準文字列生成手段によって基準文字列を生成するステップと、演算手段によって、前記基準文字列をキーとして所定の演算対象文字列を前記一方向関数により演算することにより前記ユニークコードを生成するステップとからなることを特徴とする。

第１２の発明は、第１１の発明のプログラムであって、前記演算手段によって前記ユニークコードを生成するステップは、桁数決定手段によって前記基準文字

列に基づいて演算桁数を決定するステップと、演算対象文字列生成手段によって前記演算桁数を有する演算対象文字列を生成するステップと、演算実行手段により前記基準文字列をキーとして前記演算対象文字列を前記一方向関数により演算するステップとからなることを特徴とする。

第１３の発明は、第９の発明のプログラムであって、前記情報管理用コンピュータに、二次変換データ生成手段によって前記一次変換データを暗号化して二次変換データを生成するステップと、出力手段によって前記二次変換データを他の装置へ出力するステップと、前記出力手段により前記二次変換データが出力された際に、出力された前記二次変換データと、前記二次変換データのもとになった前記一次変換データと、前記一次変換データのもとになった前記処理対象のデータと、前記出力手段による出力記録とを対応づけて記憶手段に記憶するステップとをさらに含む処理を実行させることを特徴とする。

図面の簡単な説明

第１図は、本発明の実施の形態における処理の概念を示す図である。

第２図は、本発明の実施の形態の情報管理システムの構成を示す図である。

第３図は、第２図に示す情報管理装置の機能的構成を示すブロック図である。

第４図は、本発明の実施の形態において処理されるレセプトデータの構成を示す図である。

第５図は、第２図に示す情報管理システムの動作を示すフローチャートである。

第６図は、本発明の実施の形態におけるユニークコード生成処理を詳細に示すフローチャートである。

第７図は、本発明の実施の形態におけるユニークコード生成処理を具体的な例を挙げて説明する図である。

第８図は、本発明の実施の形態におけるユニークコード生成処理を、別の具体的な例を挙げて説明する図である。

第９図は、本発明の実施の形態におけるデータ送受信処理を詳細に示すフローチャートである。

第１０図は、個人情報を含むデータを格納したデータベースの例を示す図であ

る。

第１１図は、ユニークコードを含むデータを格納したデータベースの例を示す図である。

発明を実施するための最良の形態

第１図は、本発明の実施の形態の基本的概念を示す図である。本発明は、個人情報を含むデータを処理対象とする。

ここで、個人情報とは、それ自体または他の情報と組み合わせることにより個人を特定することが可能な情報、及び、個人の履歴（学歴、職歴および個人の行動履歴を示すその他の情報を含む）、各種組織における個人の属性を示す情報等、本人の承諾を得なければ利用や公開ができない、あるいは秘匿することが好ましいとされる情報である。個人情報の具体例としては、氏名、生年月日、性別、年齢、住所、連絡先（電話番号、ファクシミリ番号、電子メールアドレス等）、社会保障や税金に関係する情報（社会保障番号、納税者番号等）、職業に関する情報（勤務先の名称、所在地、連絡先、所属部門、職責等）、在籍中または卒業した教育機関に関する情報（教育機関の名称、所在地、連絡先、入学または卒業年度、学籍番号等）、個人の購買履歴を示す情報（商品購入履歴、個人が加入する生命保険や損害保険の証券番号等）、クレジットカード番号等の個人の与信情報、金融機関の口座番号等が挙げられる。

第１図に示す基本データ１０１は、第三者が識別可能な状態で個人情報１０２を含む。本実施の形態では、個人情報１０２をもとにユニークコード１０４を生成し、個人情報１０２をユニークコード１０４に置き換えることで一次変換データ１０３を生成する。つまり、一次変換データ１０３は、基本データ１０１の個人情報１０２をユニークコード１０４に置き換えた以外は、基本データ１０１と同一のデータである。

さらに、本実施の形態では、一次変換データ１０３を他の装置へ出力する場合、すなわち通信回線を介して送受信し、或いは記録媒体等に記録して輸送する場合に、一次変換データ１０３全体を所定のパスワードで暗号化した二次変換データ１０５を用いる。二次変換データ１０５の出力を受けた装置においては、上記パ

スワードを用いて二次変換データ１０５を復号すれば、一次変換データ１０３を得ることができる。

以下、本実施の形態の好ましい具体的態様について、第２図～第１１図の各図を参照して詳細に説明する。

第２図は、本発明の実施の形態の情報管理システムの構成を示す図である。第２図に示す情報管理システム１は、情報管理装置２と、ネットワーク３を介して情報管理装置２に接続された情報センタ装置４とから構成される。なお、第２図には２台の情報管理装置２を示したが、情報管理装置２の数は１以上であれば良い。

ネットワーク３は、専用線、公衆電話回線、衛星通信回線等の各種通信回線を含んで構成される。なお、ネットワーク３は、インターネットのようなオープンなネットワークであっても良いし、限られた装置のみアクセス可能なクローズドネットワークであっても良い。また、ネットワーク３の具体的態様（回線の種類、帯域幅、ネットワークトポロジ、使用するプロトコル）については特に限定されず、各種のサーバ装置やファイアーウォール装置、ゲートウェイ装置等を含むものとしても良い。

情報管理装置２および情報センタ装置４は、ネットワーク３を介して、互いに各種データや制御情報等を送受信する。

情報センタ装置４は、情報管理装置２から送信される情報を受信し、受信した情報が暗号化されている場合は復号する。さらに、情報センタ装置４はデータベース５を備え、復号した情報をデータベース５に蓄積させるとともに、データベース５に蓄積された情報を検索し、選択（selection）、射影（projection）、結合（join）等の操作を実行する。

第３図は、情報管理装置２の機能的構成を示すブロック図である。第３図に示すように、情報管理装置２は、ＣＰＵ（Central Processing Unit）２１、ＲＡＭ（Random Access Memory）２２、記憶装置２３、記録媒体読取装置２４、入力装置２５、表示装置２６、および通信制御装置２７を備え、これらの各部はバス２８に接続されている。

ＣＰＵ２１は、入力装置２５を用いてユーザが入力した指示に基づいて、記憶装置２３に格納されたコンピュータプログラムを読み出して実行し、第５図に示す処理を実行する。すなわち、ＣＰＵ２１は、記録媒体読取装置２４によって記録媒体に記録された情報を読み取ることにより基本データを取得し、基本データから一次変換データを生成する。さらに、ＣＰＵ２１は、一次変換データを暗号化して二次変換データを生成し、ネットワーク３を介して情報センタ装置４に送信する。

ＲＡＭ２２は、ＣＰＵ２１によって実行されるコンピュータプログラムや、コンピュータプログラムの実行時に処理されるデータを一時的に格納する。

記憶装置２３は、ＣＰＵ２１によって実行されるコンピュータプログラムや、コンピュータプログラムの実行時に処理されるデータを、ＣＰＵ２１による読み取りが可能な状態で記憶している。記憶装置２３は、ＣＰＵ２１からの読み出し要求に応じて、要求されたコンピュータプログラムやデータ等をＣＰＵ２１に出力する。また、記憶装置２３は、ＣＰＵ２１からの書き込み要求に応じてデータを記憶する。

記録媒体読取装置２４は、磁気的、光学的記録媒体や半導体メモリ素子を内蔵した記録媒体等、可搬型の記録媒体に記録された情報を、ＣＰＵ２１の制御に従って読み取る装置である。

入力装置２５は、マウス、ペンタブレット、タッチパネル、ディジタイザ等のポインティングデバイス、及び、キーボード等の入力デバイスを備え、上記入力デバイスの操作に応じて操作信号を生成し、ＣＰＵ２１に出力する。

表示装置２６は、ＣＲＴ（Cathode Ray Tube）やＬＣＤ（Liquid Crystal Display）等の表示画面を有し、入力装置２５により入力された指示やＣＰＵ２１により実行された処理の結果等を上記表示画面上に表示する。

通信制御装置２７はネットワーク３に接続され、ネットワーク３を介して各種情報を送受信する。

第４図は、本実施の形態において処理対象となるレセプトデータの構成を示す図である。第４図（ａ）は、レセプトデータ全体の構成を示し、第４図（ｂ）は特に個人情報を含む部分の構成を示す図である。情報管理システム１は様々なデ

ータを処理することが可能であるが、本実施の形態では、個人情報を含むデータの一例としてレセプトデータを処理する場合について説明する。

ここで、レセプトとは、正式には診療報酬明細書といい、日本国内の医療保険制度を利用して診療報酬の支払いを受けるために、医療機関が作成して保険者に提出する書類である。レセプトには、患者自身の個人情報、患者が診療を受けた医療機関に関する情報、診療内容を示す情報、診療報酬金額に関する情報等、様々な情報が記録される。

レセプトを用いた診療報酬の請求は、通常、月ごとに行われるので、医療機関は、一人の患者に対して一ヶ月間に行った診療行為の診療報酬を、一通のレセプトにより請求する。一人の患者が複数の医療機関で診療を受けた場合、これら複数の医療機関は、それぞれレセプトを作成して提出する。従って、一人の患者について、ひと月に複数のレセプトが提出されることがある。

診療に関する情報を電子化して処理している医療機関では、レセプトに記録する情報をまとめたレセプトデータを作成し、指定された書式でレセプトデータを印刷することでレセプトを作成している。

レセプトデータは、例えば、第４図（ａ）に示すように構成される。なお、第４図（ａ）はあくまで一例を示す図であり、必ずしも全てのレセプトが第４図（ａ）のように構成されるとは限らない。

レセプトデータ６は、レセプトに記録すべき各種の情報をＣＳＶ（Comma Separated Value）形式で記述したものであり、医療機関レコード６１、レセプト共通レコード６２、保険者レコード６３、老人レコード６４、公費レコード６５、傷病名レコード６６および摘要情報６７を含んで構成される。

医療機関レコード６１は、患者が診療を受けた医療機関、すなわちレセプトを作成する医療機関に関する情報およびその他の情報を含む最大６２バイトのデータで構成される。具体的には、医療機関レコード６１は、医療機関の所在地が属する自治体、医療機関に付与されたコード、医療機関の名称、診療科目、診療報酬を請求する年月等を示す情報を含む。

レセプト共通レコード６２は、主として患者に関する情報を含む最大１２２バイトのデータで構成される。レセプト共通レコード６２は、具体的には、患者が

診療を受けた年月、患者の氏名、生年月日、性別、診療報酬のうち患者が自己負担すべき割合、カルテの番号等の情報を含み、患者が入院治療を受けた場合は、入院年月日、入院した病棟の種別、病床数等の情報を含む。

保険者レコード６３は、診療報酬の請求先の保険者に関する情報や、患者の医療保険加入者番号、診療報酬金額および内訳に関する情報等を含む最大１３８バイトのデータで構成される。

老人レコード６４は、老人医療費制度に基づいて自治体による医療費の給付を受けるために必要な各種情報を含み、最大１４３バイトのデータで構成される。

公費レコード６５は、特例的な医療費の公的補助を受けるために必要な各種情報を含み、最大６３バイトのデータで構成される。

傷病名レコード６６は、患者の傷病に関する情報を含む最大１３９バイトのデータで構成される。

摘要情報６７は、医療機関が患者に対して行った診療行為の内容等を示す情報を含む診療行為レコード（最大３２バイト）、使用した医薬品に関する情報を含む医薬品レコード（最大３３バイト）、使用した機材に関する情報を含む特定機材レコード（最大８６バイト）、及び、診療内容に関する追加的な情報であるコメント等の情報を含むコメントレコード（最大９０バイト）を含む最大２４１バイトのデータで構成される。

レセプト共通レコード６２は、第４図（ｂ）に示すように、患者の個人情報である氏名６２１（最大４０バイト）、生年月日６２２（７バイト）および性別コード６２３（１バイト）を含む。性別コードは、性別を示すコードとして予め定められたものである。本実施の形態では、男性を「１」、女性を「２」で表す。

続いて、情報管理システム１の動作について説明する。

第５図は、第２図に示す情報管理システムの動作を示すフローチャートである。第５図（ａ）は、特に情報管理装置２の動作を示し、第５図（ｂ）は情報センタ装置４の動作を示す。

ステップＳ１１（第５図（ａ））で、情報管理装置２は、記録媒体読取装置２４によって記録媒体から情報を読み取ることにより、処理対象の基本データ（レセプトデータ）を取得する。

ステップＳ１２で、情報管理装置２は基本データ中の個人情報を検出する。次に、ステップＳ１３で、情報管理装置２は、ステップＳ１２で検出した個人情報をもとにユニークコードを生成する処理を実行する。ステップＳ１３のユニークコード生成処理については、第６図を参照して後で説明する。

ユニークコード生成処理の後、ステップＳ１４で、情報管理装置２は、基本データを複製し、複製した基本データ中の個人情報をユニークコードに置き換えることによって一次変換データを生成する。ステップＳ１５で、情報管理装置２は、ステップＳ１４で生成した一次変換データを基本データとともに記憶装置２３に記憶し、ステップＳ１６に移行して、入力装置２５からの指示入力を受け付ける。

ステップＳ１６で、入力装置２５から、情報センタ装置４にデータを送信する旨の指示が入力された場合、情報管理装置２はステップＳ１７に移行し、情報センタ装置４へデータを送信する処理を実行する。ステップＳ１７のデータ送受信処理については、第９図（ａ）を参照して後で説明する。

ステップＳ１７のデータ送受信処理の後、情報管理装置２は動作を終了する。

また、ステップＳ１６において、入力装置２５から指示が入力されなかった場合、情報管理装置２はステップＳ１１に戻る。

情報センタ装置４は、情報管理装置２がステップＳ１７のデータ送受信処理を開始すると同時に、ステップＳ２１（第５図（ｂ））に移行してデータ送受信処理を実行する。ステップＳ２１のデータ送受信処理については、第９図（ｂ）を参照して後で説明する。

データ送受信処理の後、情報センタ装置４はステップＳ２２に移行し、ステップＳ２１で受信した情報について、ユニークコードをキーとして、データベースを操作する処理を行う。

第６図は、第５図（ａ）のステップＳ１３に示すユニークコード生成処理を、より詳細に示すフローチャートである。

ステップＳ３１で、情報管理装置２は基本データから個人情報を抽出する。ステップＳ３２で、情報管理装置２は、抽出した個人情報から半角スペースおよび全角スペースを除去して基準文字列を作成する。

続くステップＳ３３で、情報管理装置２は、基準文字列を構成する全ての文字

について、文字コードを取得する。なお、ステップＳ３３においては、ＡＳＣＩＩコード、Ｕｎｉｃｏｄｅ、ＪＩＳコード、シフトＪＩＳコード等の文字コードセット等の各種文字コードセットを使用することが可能である。

ステップＳ３４で、情報管理装置２は、基準文字列を構成する全ての文字の文字コードを合計する。続くステップＳ３５で、情報管理装置２は、ステップＳ３４で求めた文字コードの和を３２で除算し、商と余りを求める。情報管理装置２はステップＳ３６に移行し、求めた余りに１００を加えて演算桁数とする。

以上のステップＳ３３～ステップＳ３６の処理によって、演算桁数は、１００～１３１のいずれかに決定される。なお、演算桁数がとりうる値の範囲は、ステップＳ３５で用いる除数（法）を変化させることによって決定される。例えば、除数（法）を５０とすれば、１００～１４９の範囲で演算桁数が決定される。また、例えば除数（法）を１０とすれば１００～１０９の範囲で演算桁数が決定される。つまり、除数（法）を整数ｎとすれば、演算桁数は１００～｛１００＋（ｎ－１）｝の範囲で決定される。本実施の形態ではあくまで一例として、除数（法）に３２を用いている。

その後、情報管理装置２はステップＳ３７に移行して、演算桁数と同じ桁数を有する文字列を生成し、ＮＵＬＬクリアする。これにより、演算桁数に等しい桁数を有し、かつ、全ての桁が「0（ゼロ）」である文字列が生成される。このステップＳ３７で生成された文字列を演算対象文字列とする。

ステップＳ３８で、情報管理装置２は、演算対象文字列を、一方向ハッシュ関数によって、基準文字列をキーとして演算する。ステップＳ３８の演算が完了した後、情報管理装置２はステップＳ３９に移行し、演算結果をバイナリダンプして文字列を生成し、生成した文字列をユニークコードとする。ステップＳ３９でバイナリダンプを行うのは、ハッシュ関数を用いた演算の結果が制御コードを含む可能性があるためである。

第６図に示すユニークコード生成処理では、個人情報からスペースを除いた基準文字列の文字コードをもとに演算桁数が決定されるので、基準文字列が一文字でも異なる場合は、演算桁数が異なる。一般に、ハッシュ関数を用いた演算では、初期値の変化によって演算結果が極めて大きな影響を受けることが明らかになっ

ている。従って、演算桁数がわずかでも異なる場合、演算結果は極端に異なったものとなる。さらに、第６図に示すユニークコード生成処理では、基準文字列をキーとして演算を行うので、基準文字列が一文字でも異なっていると、演算結果に、さらに大きな差を生じる。

例えば、氏名、生年月日および性別をもとにユニークコードを生成する場合、氏名、生年月日、性別のいずれか一つの情報が、一文字だけでも違っていれば、全く異なるユニークコードが生成されるのである。従って、異なる複数の人物の個人情報から同一のユニークコードが生成される確率はゼロに近く、無視できる。

また、このように生成されたユニークコードは、それ自体は一見して無意味な文字列にしか見えないので、多数のユニークコードを分析しても何ら規則性を発見することはできない。このため、ユニークコードを演算して個人情報を得ることは実質的に不可能であり、そのユニークコードが、氏名のみを基準文字列として生成されたのか、氏名と生年月日を含む基準文字列から生成されたのかを判別することも不可能である。

このように、ユニークコードは、個人情報をもとに生成されるにも関わらず、ユニークコード自体から個人情報を知る手段がないので、一次変換データのみを利用する限りにおいて、個人情報が漏洩する恐れはない。

さらに、第６図に示す処理においては、個人情報からスペースを除去した後にユニークコードを生成するので、スペースの使い方等の表記方法の違いにも対応することができる。なお、第６図のステップＳ３２では全角および半角のスペースを除去するものとしたが、例えば、個人情報中にアルファベットの大文字と小文字とが混在する場合に、全てのアルファベットを小文字に変換する処理を行っても良い。

さらに、同一人物の個人情報から、意図的に異なる複数のユニークコードを生成することも可能である。すなわち、氏名と生年月日のみを基準文字列とした場合のユニークコードと、氏名、生年月日および性別を基準文字列とした場合のユニークコードは異なるものになる。このため、特定の個人について、個人情報とこの個人情報をもとに生成したユニークコードとの対応関係が漏洩してしまった場合は、基準文字列の内容を変えて新たなユニークコードを生成すれば、それ以

上の個人情報の漏洩を防ぐことができる。また、基本データの形態やユニークコードの用途に応じて、適宜、異なるユニークコードを生成することにより、ユニークコード生成処理の処理速度を高めることも、ユニークコードをさらに複雑化することも可能であり、効率よくユニークコードを利用することができる。

第７図は、第６図に示すユニークコード生成処理を、具体的な例を挙げて説明する図である。第７図の例では、１９７０年５月１５日生まれの山田太郎という男性の個人情報からユニークコードを生成する。

情報管理装置２によって抽出される個人情報は、氏名「山田　太郎」、生年月日「19700515」および性別コード「1」である。情報管理装置２によって半角および全角のスペースが除去されると、基準文字列「山田太郎197005151」が作成される。基準文字列には漢字４文字で構成される日本語の人名が含まれるので、情報管理装置２は、シフトＪＩＳ文字コードセット等の日本語用文字コードセットを用いて文字コードを取得する。日本語用文字コードセットでは漢字は２バイト文字として扱われるので、４文字の漢字から各々２バイトの文字コードが得られる。また、上記日本語用文字コードセットでは半角数字は１バイト文字として扱われるので、「197005151」の９文字から各々１バイトの文字コードが得られる。これにより、基準文字列「山田太郎197005151」から１７バイトの文字コードが得られる。

次に、情報管理装置２によって、基準文字列の文字コードが合計される。第７図に示すように「8E+52+93+63+91+BE+98+59+31+39+37+30+30+35+31+35+31＝5E3(１６進数表記)」の演算が情報管理装置２によって行われ、文字コードの和「5E3」が求められる。「5E3」は１０進数で表記すると「1507」である。続いて、情報管理装置２によって、文字コードの和「1507」が「32」で除算され、商が「47」、余りが「3」と求められる。演算桁数は、余りの「3」に「100」を加えて１０３桁に決定される。その後、情報管理装置２によって全ての桁が「0（ゼロ）」で構成される１０３桁の演算対象文字列が生成され、基準文字列「山田太郎197005151」をキーとしてハッシュ関数による演算が行われる。演算結果はバイナリダンプされ、例えば、ユニークコード「69654665019b733fe725353a5884fd94469d85e857820ad6742c3fc1b1b2e1ec3ee38c2e63b541c7b11f0781cda5a82838b0d5e5b3

2eceffeec6bd484356b69c97498dbdf54e706719ecc7d90db8254762b4437b429fb6184
3c009b1b9f5ec3d7b6085b5548b1」が生成される。なお、このユニークコードは、セキュリティ上の配慮から、実際に上記基準文字列をもとに得られるユニークコードの一部を改変したものである。

第８図は、第６図に示すユニークコード生成処理を、別の具体的な例を挙げて説明する図である。第８図の例では、１９７０年２月２６日生まれのＮａｎｃｙＬｏｐｅｚという女性の個人情報からユニークコードを生成する。

情報管理装置２によって抽出される個人情報は、氏名「Nancy Lopez」、生年月日「19700226」および性別コード「2」である。情報管理装置２によって半角および全角のスペースが除去されると、基準文字列「NancyLopez197002262」が作成される。半角の英数字は、各種文字コードセットにおいて１バイト文字として扱われるので、基準文字列「NancyLopez197002262」からは、１９バイトの文字コードが得られる。

次に、情報管理装置２によって、基準文字列の文字コードが合計される。第８図に示すように「4E+61+6E+63+79+52+6F+70+65+7A+31+39+37+30+30+32+32+36+32＝5DB(１６進数表記)の演算が情報管理装置２によって行われ、文字コードの和「5DB」が求められる。「5DB」は１０進数で表記すると「1499」である。続いて、情報管理装置２によって、文字コードの和「1499」が「32」で除算され、商が「46」、余りが「27」と求められる。演算桁数は、余りの「27」に「100」を加えて１２７桁に決定される。その後、情報管理装置２によって全ての桁が「0（ゼロ）」で構成される１２７桁の演算対象文字列が生成され、基準文字列「NancyLopez197002262」をキーとしてハッシュ関数による演算が行われる。演算結果はバイナリダンプされ、例えば、ユニークコード「56b03813bad4c752a5c13247a0bc194ca607caf2e295646a061027d09c00d9ec9767f6e825c521647b16a19df9ee6041ae400b7fa1026c93491d1d577a815129626493b6e9da791e85203fd00018e6022a0215afb571b67fffd47d3e687dad79252ad98012bdd73d476edc0639a73cd9ca2a7f3c831e065bdd」が生成される。なお、このユニークコードは、セキュリティ上の配慮から、実際に上記基準文字列をもとに得られるユニークコードの一部を改変したものである。

第９図は、本発明の実施の形態のデータ送受信処理をより詳細に示すフローチ

ャートである。第９図（ａ）は第５図（ａ）のステップＳ１７で情報管理装置２が実行する処理を示し、第９図（ｂ）は第５図（ｂ）のステップＳ２１で情報センタ装置４が実行する処理を示す。

この第９図に示すデータ送受信処理では、ＤＨ（Diffie-Hellman）方式による公開鍵の交換を行って、一次変換データを送受信する。

ステップＳ４１（第９図（ａ））で、情報管理装置２は、例えば乱数を用いて秘密鍵ＰＲ１を生成する。ステップＳ４２で、情報管理装置２は、所定の演算式を用いて秘密鍵ＰＲ１から公開鍵ＰＵ１を生成する。そして、ステップＳ４３で、情報管理装置２は、公開鍵ＰＵ１をネットワーク３を介して情報センタ装置４に送信するとともに、情報センタ装置４から送信される公開鍵ＰＵ２を受信する。

一方、情報センタ装置４は、ステップＳ５１（第９図（ｂ））で秘密鍵ＰＲ２を、例えば乱数を用いて生成し、ステップＳ５２で、所定の演算式を用いて秘密鍵ＰＲ２から公開鍵ＰＵ２を生成する。そして、情報センタ装置４は、ステップＳ５３で、公開鍵ＰＵ２をネットワーク３を介して情報管理装置２に送信するとともに、情報管理装置２から送信される公開鍵ＰＵ１を受信する。

以上のステップＳ４１～Ｓ４３及びステップＳ５１～Ｓ５３の処理により、情報管理装置２と情報センタ装置４とは、自己が生成した秘密鍵と、相手が生成した公開鍵とを保持することになる。なお、情報管理装置２と情報センタ装置４との間で、以上のステップＳ４１～Ｓ４３及びステップＳ５１～Ｓ５３の処理を行っておいてから、第５図に示す処理を行っても良い。すなわち、第５図の処理を行うに先立って、予め、情報管理装置２と情報センタ装置４とが、自己が生成した秘密鍵と相手が生成した公開鍵とを保持している構成としても良い。この場合、公開鍵ＰＵ１および公開鍵ＰＵ２は、ネットワーク３を介して送受信しても良いし、入力装置２５等による入力操作や可搬型の記録媒体を用いて、情報管理装置２及び情報センタ装置４に入力されても良い。

ステップＳ４４（第９図（ａ））で、情報管理装置２は、自己が生成した秘密鍵ＰＲ１と情報センタ装置４から受信した公開鍵ＰＵ２とをもとに、共通鍵ＣＫを生成する。

ステップＳ４５で、情報管理装置２は、セッション鍵ＳＫを生成する。続くス

テップＳ４６で、情報管理装置２は、セッション鍵ＳＫを用いて一次変換データを暗号化することにより、二次変換データを生成する。

さらに、情報管理装置２はステップＳ４７に移行して、セッション鍵ＳＫを共通鍵ＣＫによって暗号化し、ステップＳ４８で、暗号化したセッション鍵ＳＫを二次変換データに付加して情報センタ装置４へ送信する。

その後、ステップＳ４９で、情報管理装置２は、情報センタ装置４への送信結果を示す送信ログを作成して、二次変換データと送信ログを、記憶装置２３に記憶された基本データおよび一次変換データに対応づけて記憶装置２３に記憶し、処理を終了する。

一方、情報センタ装置４は、ステップＳ５５（第９図（ｂ））で、暗号化されたセッション鍵ＳＫと二次変換データとを受信する。続くステップＳ５６で、情報センタ装置４は、受信したセッション鍵ＳＫを、ステップＳ５４で生成した共通鍵ＣＫにより復号し、ステップＳ５７で、復号したセッション鍵ＳＫにより二次変換データを復号して一次変換データを得る。

ステップＳ５８で、情報センタ装置４は、ステップＳ５７で得られた一次変換データをデータベース５に登録し、処理を終了する。

第１０図は、個人情報を含むデータを格納したデータベースの例を示す図である。第１０図に例示するデータベースは、個人の氏名、生年月日、性別コード、医療機関名、傷病名、診療日数、診療内容の各項目のデータを含むレコードを格納するものであって、複数の個人に関する複数のレコードを格納している。

このように、個人情報を含むデータをデータベース化すると、個人情報をキーとして、選択、射影、結合等のデータベース操作を行い、個人毎にデータを抽出することが可能である。しかしながら、個人情報を格納したデータベースは個人情報の保護のための方策を施す必要がある。

そこで、第１０図に示すデータベースに格納されるレコードを、個人情報の代わりにユニークコードを含む一次変換データに置き換えた例を、第１１図に示す。

第１１図に例示するデータベースは、ユニークコードを含む複数のレコードを格納している。第１１図に示すデータベースは個人情報を含まないため、個人情報を保護するための特別な方策は不要である。

さらに、第１１図に示すデータベースにおいては、ユニークコードをキーとして、個人毎にデータを操作することが可能である。例えば、第１１図に示すように、ユニークコード「548b1695d8e9a2b6085b5」をキーとして選択操作を行うと、Ｎｏ．１とＮｏ．４の二つのレコードが抽出される。抽出された二つのレコードは、ユニークコードが同一であることから同一人物に関するレコードであることがわかる。従って、第１０図に示すデータベースを、第１１図に示すデータベースに置き換えても、情報の検索容易性は損なわれない。

このように、本実施の形態では、個人情報をユニークコードに置き換えた一次変換データを用いることにより、情報の有用性を損なうことなく、個人情報を確実に保護することが可能である。

以上のように、本実施の形態における情報管理システム１によれば、個人情報を含む処理対象のデータをそのままデータベース化せず、処理対象のデータ（基本データ）中の個人情報からユニークコードを生成し、個人情報をユニークコードに置き換えた一次変換データを生成して、一次変換データをデータベース５に格納して統計的処理に用いる。ユニークコードは、個人情報からスペースを除去した基準文字列をもとに、一方向ハッシュ関数を用いた演算により生成されるので、逆の演算を行ってもとの個人情報を知ることがほぼ不可能である。このため、一次変換データを処理する過程において、個人情報が漏洩する心配が全くない。

また、一方向ハッシュ関数の、演算結果が初期値の変化に極端に影響されるという特徴により、基準文字列が異なる場合、すなわち別の個人情報を用いた場合には、必ずといっていいほど別の、著しく異なるユニークコードが生成される。つまり、別人の個人情報から同一のユニークコードが生成される可能性は極めて低く、無視できる程度であり、一次変換データの有用性を高いレベルで保つことができる。さらに、ユニークコードは、基準文字列をもとに演算桁数を決定し、この演算桁数の演算対象文字列を、基準文字列をキーとして演算することにより生成されるので、基準文字列が異なる場合には、著しく異なるユニークコードが生成されるので、別人の個人情報から同一のユニークコードが生成される可能性が一段と低くなり、一次変換データの有用性を、より一層高いレベルで保つことができる。

従って、ユニークコードは、個人情報と同様に、一人の個人に対して固有の値となるので、ユニークコードを含む多数のデータを、個人毎に検索、抽出する操作に利用することができる。このように、個人情報の代わりにユニークコードを含む一次変換データは、個人情報を含むデータと同等の有用性があり、統計的処理に活用できる。そして、この一次変換データを用いることにより、個人情報を含むデータを処理する際に、情報の有用性を損なうことなく、個人情報を確実に隠蔽して保護することができる。そして、情報管理システム１は、情報管理装置２によって、基本データから一次変換データを効率よく生成することができる。

また、情報管理装置２は、基本データから一次変換データを生成した場合には一次変換データと、もとになった基本データとを対応づけて記憶装置２３に記憶する。さらに、一次変換データから二次変換データを生成して情報センタ装置４へ送信した場合には、二次変換データと、この二次変換データのもとになった一次変換データと、この一次変換データのもとになった基本データと、送信記録とを対応づけて記憶装置２３に記憶するので、情報管理装置２における一次変換データの生成、二次変換データの生成および送信の履歴を示す情報を記憶することで、個人情報の流通管理を確実に行うことができる。

また、情報管理装置２から情報センタ装置４へ一次変換データを送信する際に、ＤＨ方式の鍵交換を行った上、一次変換データを暗号化して二次変換データを生成し、生成した二次変換データを、ネットワーク３を介して送信する。このため、ネットワーク３を介して情報を送信する間も、セキュリティ上の信頼性を確保することができる。さらに、万が一、一次変換データが第三者に漏洩しても、個人情報が知られる可能性は全く無いので、高い信頼性を確保できる。

さらに、情報センタ装置４は、情報管理装置２から受信した一次変換データをデータベース５に格納し、データベース５に格納された複数の一次変換データについて、ユニークコードをキーとして検索等の処理操作を行うことができ、例えば、同一のユニークコードを含む一次変換データを抽出する、いわゆる名寄せ処理を行うことも可能である。これにより、情報センタ装置４は、個人情報が漏洩する恐れが全く無い状態で、正確な統計的処理を実行することが可能となる。

なお、上記実施の形態においては、情報管理システム１の処理対象のデータと

してレセプトデータを用いる例について説明したが、本発明はこれに限定されるものではなく、例えば、金融機関の口座番号、口座名義人、預金残高や取引記録に関するデータを処理することも可能であるし、教育機関において生徒・学生の氏名と成績表とを含むデータを処理することも可能である。

また、上記実施の形態においては、情報管理装置２が基本データを取得する際に記録媒体読取装置２４を用いる構成としたが、本発明はこれに限定されるものではなく、入力装置２５からの入力によって、基本データを取得するようにしても良い。さらに、情報管理装置２を、記録媒体読取装置２４に代えて可搬型の記録媒体に対し情報を書き込むことが可能な記録媒体読取／書込装置を備える構成とし、情報センタ装置４を、情報管理装置２によって情報が書き込まれた可搬型の記録媒体から情報を読み取るための読取装置を備える構成としても良い。この場合、情報管理装置２から情報センタ装置４へ二次変換データを送る際に、ネットワーク３を用いないで、情報管理装置２の記録媒体読取／書込装置によって可搬型の記録媒体に二次変換データを書き込み、情報センタ装置４の読取装置によって、可搬型の記録媒体に書き込まれた二次変換データを読み取るといった方法を利用することができる。

その他の点においても、上記実施の形態の構成を適宜変更することは可能である。すなわち、上記実施の形態はあくまで一例であり、本発明の適用範囲を制限するものではない。

産業上の利用可能性

以上の説明から明らかなように、本発明によれば、以下に述べる効果が得られる。

（１）第１の発明によれば、個人情報を含むデータを処理する情報管理装置において、処理対象のデータから個人情報抽出手段によって個人情報を抽出し、ユニークコード生成手段により、個人情報抽出手段により抽出された個人情報をもとに一方向関数を用いた演算を行ってユニークコードを生成し、一次変換データ生成手段により、処理対象のデータ中の個人情報をユニークコードに置き換えて一次変換データを生成する。ここで生成されるユニークコードは、逆の演算を行っ

てもとの個人情報を知ることがほぼ不可能であり、かつ、異なる個人情報からは、必ずといっていいほど異なるユニークコードが生成される。従って、個人情報の代わりにユニークコードを含む一次変換データは、個人情報を含むデータと比較して同等の有用性があり、統計的処理に活用できる。そして、この一次変換データを用いることにより、個人情報を含むデータを処理する際に、情報の有用性を損なうことなく、個人情報を確実に隠蔽して保護することができる。そして、第１の発明により、上記一次変換データを効率よく生成することができる。

（２）第２の発明によれば、第１の発明の情報管理装置において、一次変換データと、この一次変換データのもとになった処理対象のデータとを対応づけて記憶手段に記憶する。従って、情報管理装置において、個人情報を含む処理対象のデータと、ユニークコードを含む一次変換データとを保存しておくことができる。

（３）第３の発明によれば、第１の発明の情報管理装置において、ユニークコード生成手段は、個人情報抽出手段により抽出された個人情報から基準文字列生成手段によって基準文字列を生成し、演算手段によって、基準文字列をキーとして、所定の演算対象文字列を一方向関数により演算することによって、ユニークコードを生成する。これにより、基準文字列が異なる場合、すなわち別の個人情報を用いた場合には、必ずといっていいほど別のユニークコードが生成される。つまり、別人の個人情報から同一のユニークコードが生成される可能性は無視できる程度であり、一次変換データの有用性を高いレベルで保つことができる。

（４）第４の発明によれば、第３の発明の情報管理装置において、演算手段は、桁数決定手段によって基準文字列に基づいて演算桁数を決定し、演算対象文字列生成手段によって演算桁数を有する演算対象文字列を生成し、演算実行手段によって、基準文字列をキーとして演算対象文字列を一方向関数により演算する。これにより、基準文字列が異なる場合には、著しく異なるユニークコードが生成されるので、別人の個人情報から同一のユニークコードが生成される可能性が一段と低くなり、一次変換データの有用性を、より一層高いレベルで保つことができる。

（５）第５の発明によれば、第１の発明の情報管理装置において、二次変換データ生成手段により、一次変換データを暗号化して二次変換データを生成し、出力

手段によって二次変換データを他の装置へ出力し、出力手段により二次変換データが出力された際に、出力された二次変換データと、二次変換データのもとになった一次変換データと、一次変換データのもとになった処理対象のデータと、出力手段による出力記録とを対応づけて記憶手段に記憶する。従って、情報管理装置において、個人情報を含む処理対象のデータと、ユニークコードを含む一次変換データと、二次変換データと、二次変換データの送信記録とを、確実に保存しておくことができる。

（6）第6の発明によれば、個人情報を含むデータを処理する情報管理装置と、情報管理装置により処理されたデータを管理する情報センタ装置とが通信回線を介して接続されてなる情報管理システムにおいて、情報管理装置は、個人情報抽出手段によって、処理対象のデータから個人情報を抽出し、ユニークコード生成手段により、個人情報抽出手段により抽出された個人情報をもとに一方向関数を用いた演算を行ってユニークコードを生成し、一次変換データ生成手段により、処理対象のデータ中の個人情報をユニークコードに置き換えて一次変換データを生成し、二次変換データ生成手段により、一次変換データを暗号化して二次変換データを生成し、生成した二次変換データを、出力手段によって通信回線を介して情報管理装置に出力し、出力手段により二次変換データが出力された際に、出力された二次変換データと、この二次変換データのもとになった一次変換データと、この一次変換データのもとになった処理対象のデータと、出力手段による出力の記録とを対応づけて記憶手段に記憶する。また、情報センタ装置は、受信手段によって情報管理装置から送信された二次変換データを受信し、復号手段により、受信手段によって受信された二次変換データを復号して一次変換データを生成する。これにより、第1の発明により得られる効果に加えて、情報管理装置から情報センタ装置へ、一次変換データを暗号化して送信することによって、セキュリティ上の信頼性を確保することができる。そして、情報管理装置とは別の装置である情報センタ装置に、一次変換データのみを送信するので、情報センタ装置に情報を送信する間、および、情報センタ装置において情報を処理する過程において、個人情報が漏洩する可能性を無くすことができる。

（7）第7の発明は、第6の発明の情報管理システムにおいて、情報センタ装置

は、復号手段により生成された一次変換データを格納するデータ格納手段をさらに備え、データ格納手段に格納されたデータを、ユニークコードをキーとして処理する。これにより、データ格納手段には、個人情報を含まない一次変換データが格納されたデータ格納手段を用いて各種の統計的な処理を行うことができる。従って、個人情報を確実に保護しながら、個人情報を含むデータを用いた場合と同等の正確なデータ処理が行える。

（８）第８の発明は、第７の発明の情報管理システムにおいて、情報センタ装置は、データ格納手段に格納された、ユニークコードを含む複数のデータの中から、同一のユニークコードを含むデータを検出する。すなわち、個人情報を含む複数のデータに対して個人情報をキーとして検出処理を行うのと同様に、個人情報を含まない複数の一次変換データに対して、ユニークコードをキーとして検索を行う。これにより、個人情報を用いることなく、同一人に係るデータと別の人に係るデータとを区別してデータを処理することが可能となる。

（９）第９の発明によれば、上記第１の発明と同一の効果が得られる。

（１０）第１０の発明によれば、上記第２の発明と同一の効果が得られる。

（１１）第１１の発明によれば、上記第３の発明と同一の効果が得られる。

（１２）第１２の発明によれば、上記第４の発明と同一の効果が得られる。

（１３）第１３の発明によれば、上記第５の発明と同一の効果が得られる。

請求の範囲

1．個人情報を含むデータを処理する情報管理装置であって、
処理対象のデータから個人情報を抽出する個人情報抽出手段と、
前記個人情報抽出手段により抽出された個人情報をもとに一方向関数を用いた演算を行ってユニークコードを生成するユニークコード生成手段と、
前記処理対象のデータ中の個人情報を前記ユニークコードに置き換えて一次変換データを生成する一次変換データ生成手段と、
を備えることを特徴とする情報管理装置。

2．前記一次変換データと、前記一次変換データのもとになった前記処理対象のデータとを対応づけて記憶する記憶手段をさらに備えることを特徴とする請求項1記載の情報管理装置。

3．前記ユニークコード生成手段は、前記個人情報抽出手段により抽出された個人情報から基準文字列を生成する基準文字列生成手段と、前記基準文字列をキーとして、所定の演算対象文字列を前記一方向関数により演算することによって、前記ユニークコードを生成する演算手段とを備えて構成されることを特徴とする請求項1記載の情報管理装置。

4．前記演算手段は、前記基準文字列に基づいて演算桁数を決定する桁数決定手段と、前記演算桁数を有する演算対象文字列を生成する演算対象文字列生成手段と、前記基準文字列をキーとして前記演算対象文字列を前記一方向関数により演算する演算実行手段とを備えて構成されることを特徴とする請求項3記載の情報管理装置。

5．前記一次変換データを暗号化して二次変換データを生成する二次変換データ生成手段と、前記二次変換データを他の装置へ出力する出力手段と、前記出力手段により前記二次変換データが出力された際に、出力された前記二次変換データと、前記二次変換データのもとになった前記一次変換データと、前記一次変換データのもとになった前記処理対象のデータと、前記出力手段による出力記録とを対応づけて記憶する記憶手段と、をさらに備えることを特徴とする請求項1記載の情報管理装置。

6．個人情報を含むデータを処理する情報管理装置と、前記情報管理装置により処理されたデータを管理する情報センタ装置とが通信回線を介して接続されてなる情報管理システムであって、

前記情報管理装置は、

処理対象のデータから個人情報を抽出する個人情報抽出手段と、

前記個人情報抽出手段により抽出された個人情報をもとに一方向関数を用いた演算を行ってユニークコードを生成するユニークコード生成手段と、

前記処理対象のデータ中の個人情報を前記ユニークコードに置き換えて一次変換データを生成する一次変換データ生成手段と、

前記一次変換データを暗号化して二次変換データを生成する二次変換データ生成手段と、

前記二次変換データを、前記通信回線を介して前記情報管理装置に出力する出力手段と、

前記出力手段により前記二次変換データが出力された際に、出力された前記二次変換データと、前記二次変換データのもとになった前記一次変換データと、前記一次変換データのもとになった前記処理対象のデータと、前記出力手段による出力の記録とを対応づけて記憶する記憶手段とを備え、

前記情報センタ装置は、前記情報管理装置から送信された二次変換データを受信する受信手段と、

前記受信手段により受信された二次変換データを復号して前記一次変換データを生成する復号手段とを備えること、を特徴とする情報管理システム。

7．前記情報センタ装置は、前記復号手段により生成された一次変換データを格納するデータ格納手段をさらに備え、

前記データ格納手段に格納されたデータを、前記ユニークコードをキーとして処理することを特徴とする請求項6記載の情報管理システム。

8．前記情報センタ装置は、前記データ格納手段に格納された、前記ユニークコードを含む複数のデータの中から、同一のユニークコードを含むデータを検出することを特徴とする請求項7記載の情報管理システム。

9．個人情報を含むデータを処理する情報管理用コンピュータに、

個人情報抽出手段によって処理対象のデータから個人情報を抽出するステップと、ユニークコード生成手段により、前記個人情報抽出手段によって抽出された個人情報をもとに一方向関数を用いた演算を行ってユニークコードを生成するステップと、

一次変換データ生成手段により、前記処理対象のデータ中の個人情報を前記ユニークコードに置き換えて一次変換データを生成するステップと、

を含む処理を実行させるためのプログラム。

１０．前記情報管理用コンピュータに、前記一次変換データと、前記一次変換データのもとになった前記処理対象のデータとを対応づけて記憶手段に記憶するステップをさらに含む処理を実行させることを特徴とする請求項９記載のプログラム。

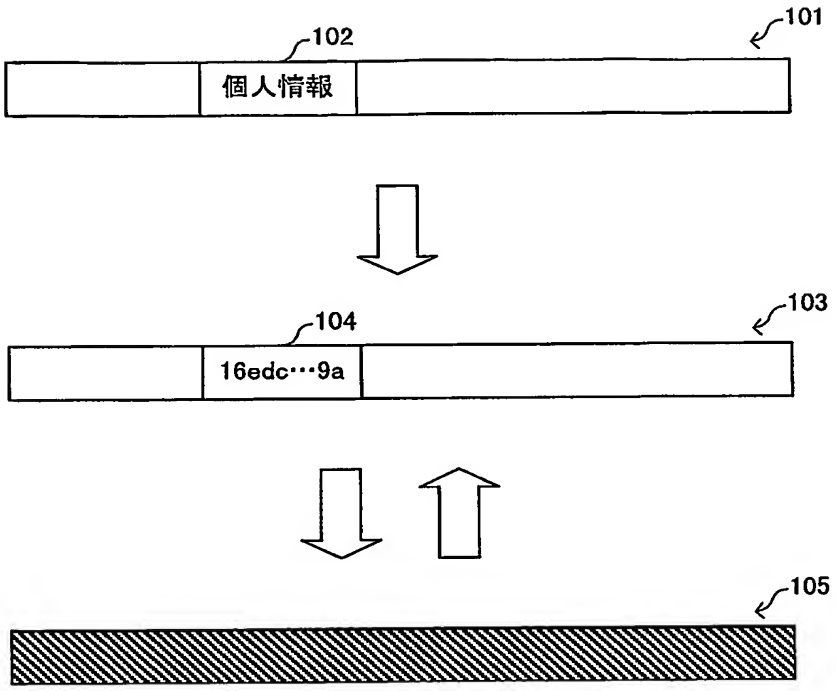
１１．前記ユニークコード生成手段によりユニークコードを生成するステップは、前記個人情報抽出手段により抽出された個人情報から基準文字列生成手段によって基準文字列を生成するステップと、演算手段によって、前記基準文字列をキーとして所定の演算対象文字列を前記一方向関数により演算することにより前記ユニークコードを生成するステップとからなることを特徴とする請求項９記載のプログラム。

１２．前記演算手段によって前記ユニークコードを生成するステップは、桁数決定手段によって前記基準文字列に基づいて演算桁数を決定するステップと、演算対象文字列生成手段によって前記演算桁数を有する演算対象文字列を生成するステップと、演算実行手段により前記基準文字列をキーとして前記演算対象文字列を前記一方向関数により演算するステップとからなることを特徴とする請求項１１記載のプログラム。

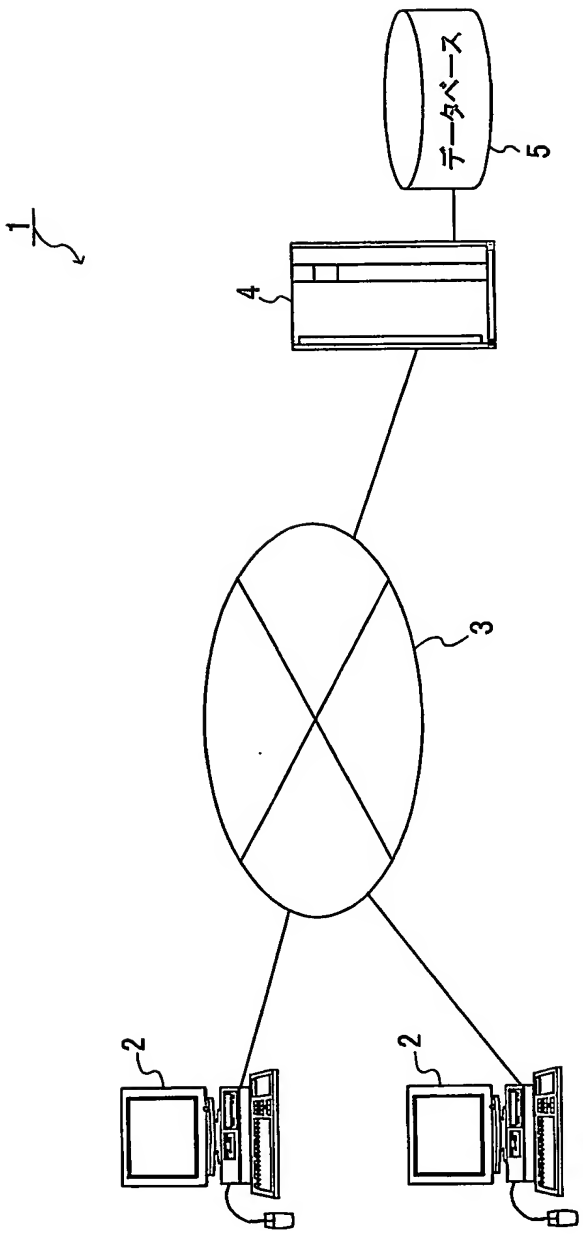
１３．前記情報管理用コンピュータに、二次変換データ生成手段によって前記一次変換データを暗号化して二次変換データを生成するステップと、出力手段によって前記二次変換データを他の装置へ出力するステップと、前記出力手段により前記二次変換データが出力された際に、出力された前記二次変換データと、前記二次変換データのもとになった前記一次変換データと、前記一次変換データのもとになった前記処理対象のデータと、前記出力手段による出力記録とを対応づけ

て記憶手段に記憶するステップとをさらに含む処理を実行させることを特徴とする請求項９記載のプログラム。

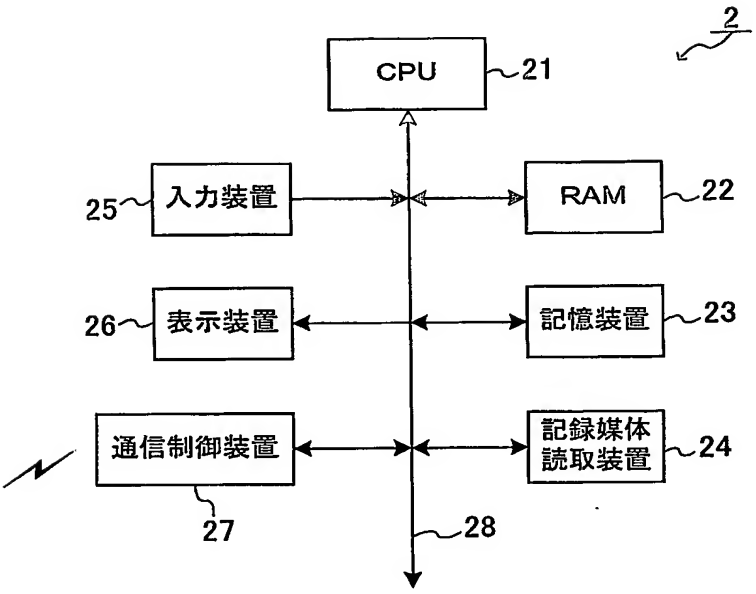
第1図



第2図

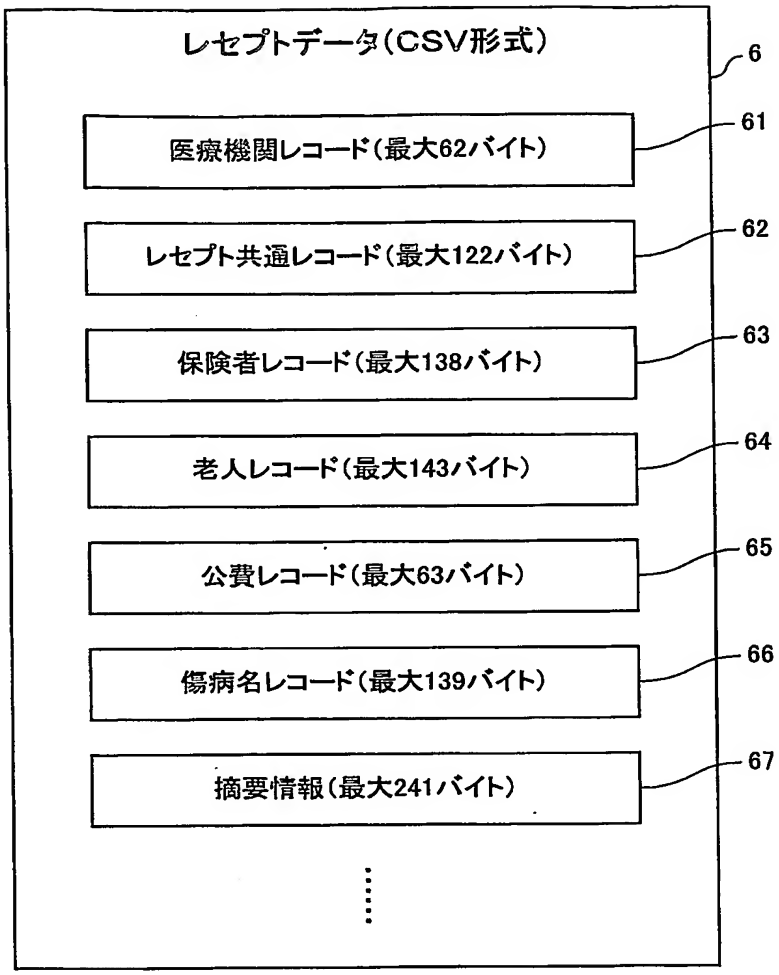


第3図

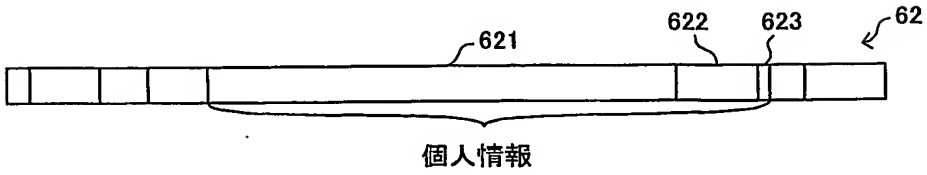


第4図

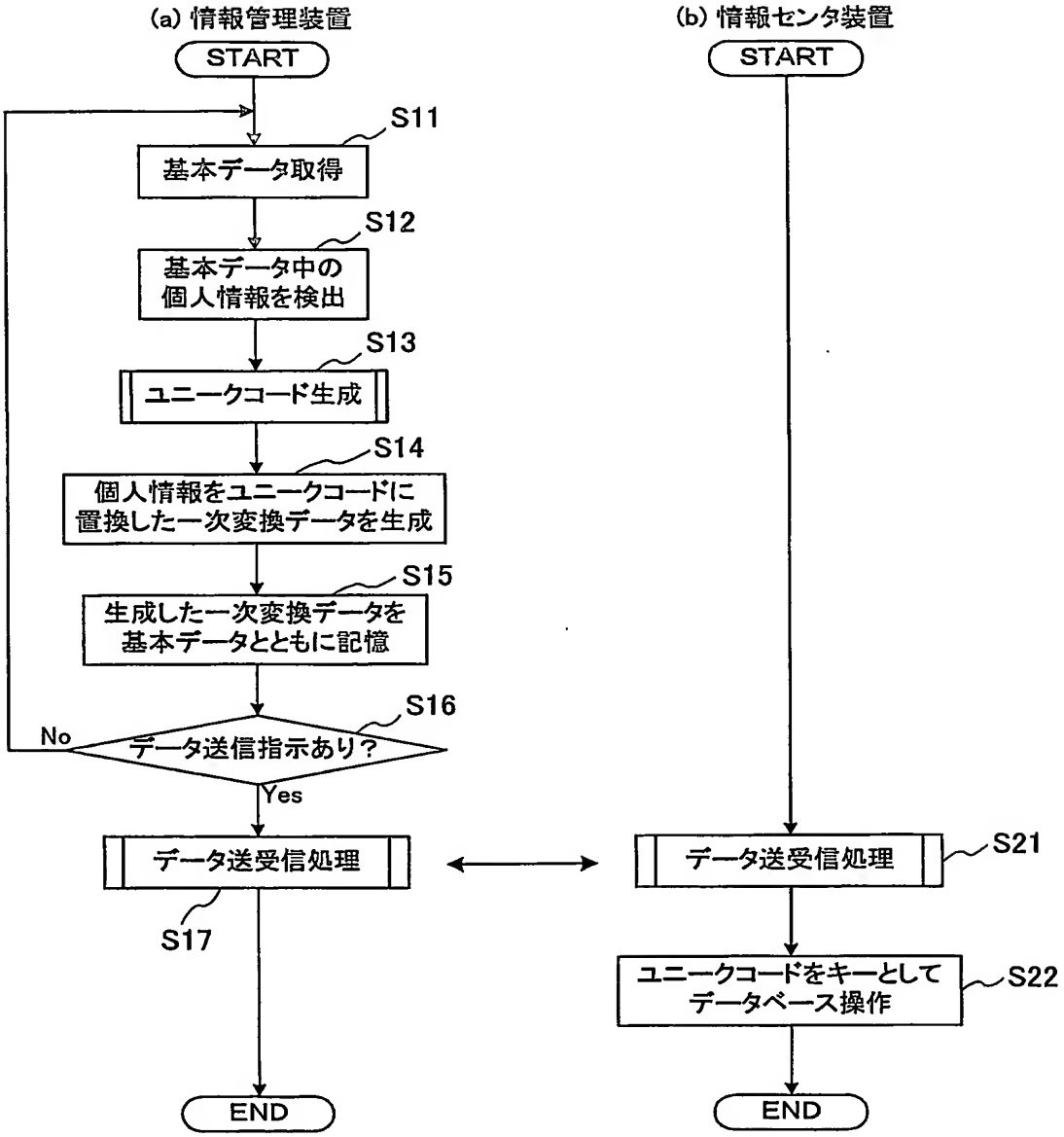
(a)


レセプトデータ(CSV形式)
6
医療機関レコード(最大62バイト)
61
レセプト共通レコード(最大122バイト)
62
保険者レコード(最大138バイト)
63
老人レコード(最大143バイト)
64
公費レコード(最大63バイト)
65
傷病名レコード(最大139バイト)
66
摘要情報(最大241バイト)
67

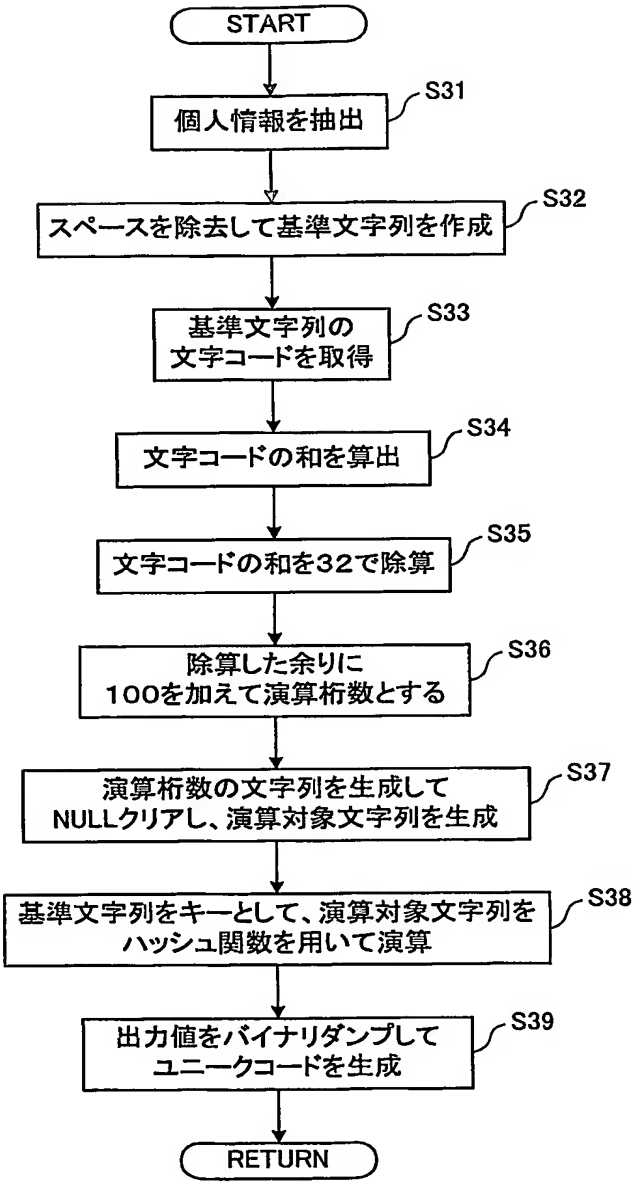
(b)


621
622
623
62
個人情報

第5図


(a) 情報管理装置
START
S11
基本データ取得
S12
基本データ中の
個人情報を検出
S13
ユニークコード生成
S14
個人情報をユニークコードに
置換した一次変換データを生成
S15
生成した一次変換データを
基本データとともに記憶
S16
No
データ送信指示あり？
Yes
データ送受信処理
S17
END
(b) 情報センタ装置
START
データ送受信処理
S21
ユニークコードをキーとして
データベース操作
S22
END

第6図


START
個人情報を抽出
S31
スペースを除去して基準文字列を作成
S32
基準文字列の
文字コードを取得
S33
文字コードの和を算出
S34
文字コードの和を32で除算
S35
除算した余りに
100を加えて演算桁数とする
S36
演算桁数の文字列を生成して
NULLクリアし、演算対象文字列を生成
S37
基準文字列をキーとして、演算対象文字列を
ハッシュ関数を用いて演算
S38
出力値をバイナリダンプして
ユニークコードを生成
S39
RETURN

第7図

氏名:山田　太郎
生年月日:1970515
性別コード:1

↓

山田太郎197005151

↓

文字	山		田		太		郎		1	9	7	0	0	5	1	5	1
文字コード	8E	52	93	63	91	BE	98	59	31	39	37	30	30	35	31	35	31

↓

8E+52+93+63+91+BE+98+59+31+39+37+30+30+35+31+35+31 ＝ 5E3(Hex)
＝1507(Dec)

↓

1507÷32＝47、余り3

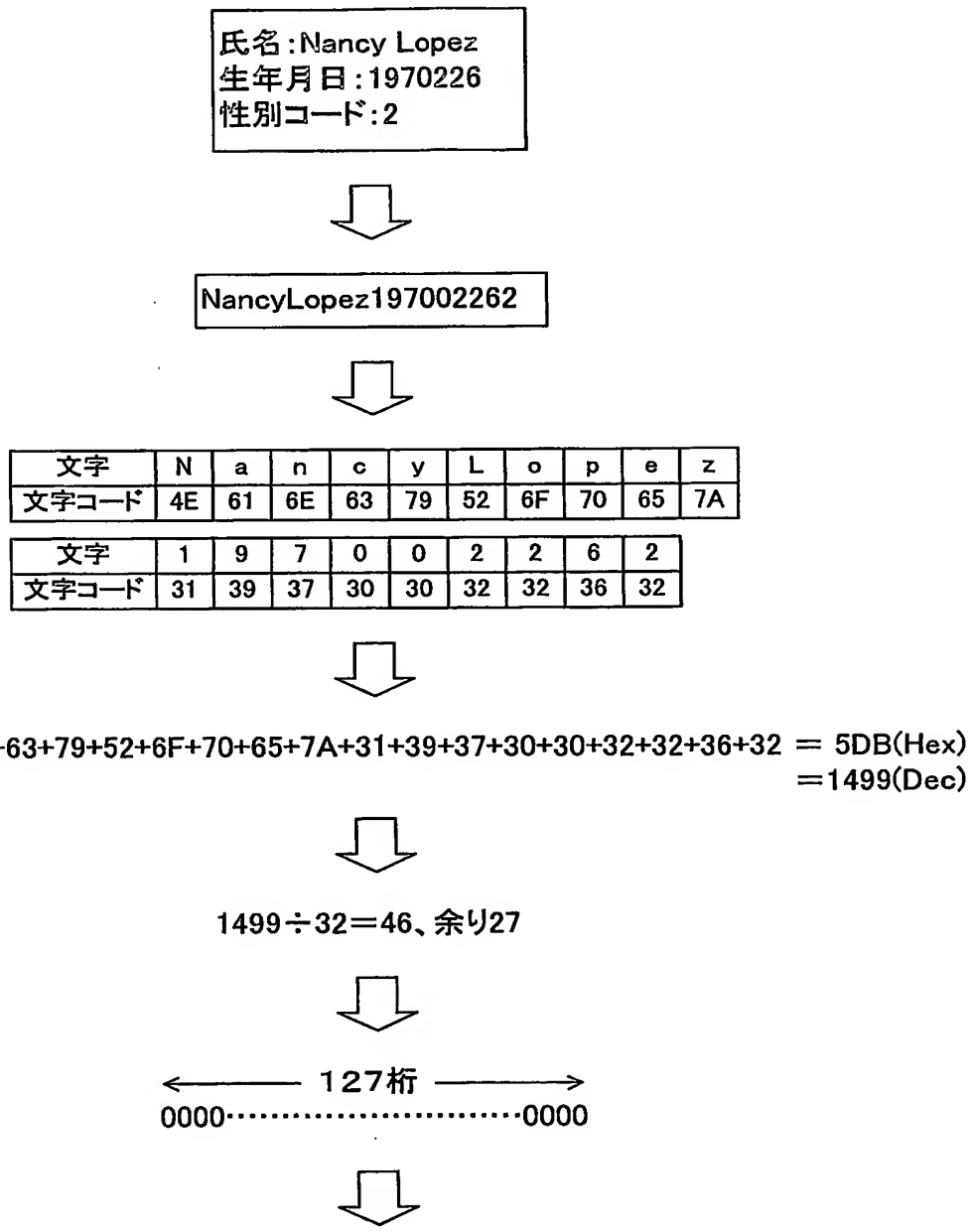
↓

←―― 103桁 ――→
0000……0000

↓

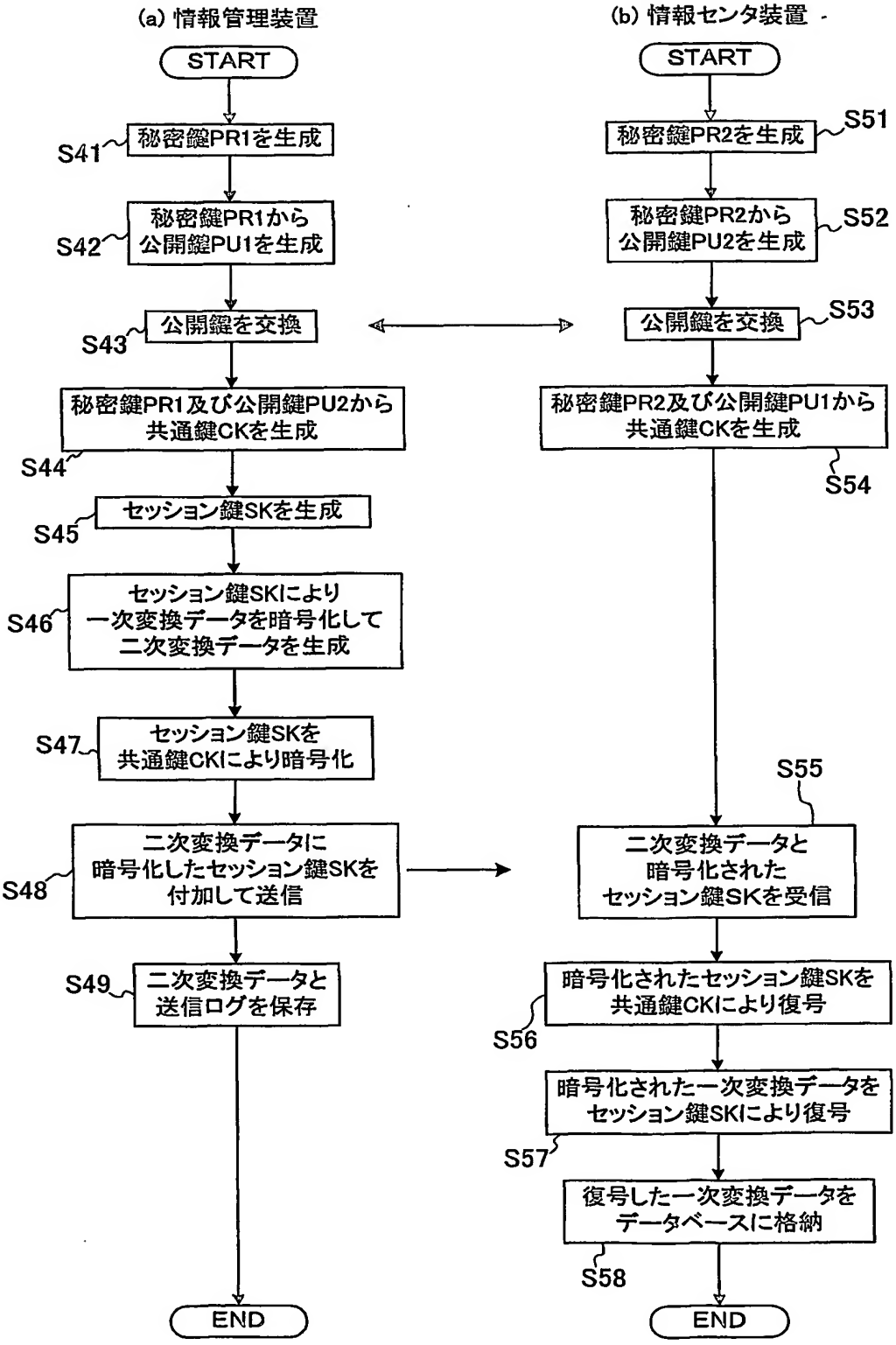
69654665019b733fe725353a5884fd94469d85e857820a
d6742c3fc1b1b2e1ec3ee38c2e63b541c7b11f0781cda5
a82838b0d5e5b32ecefffeec6bd484356b69c97498dbdf5
4e706719ecc7d90db8254762b4437b429fb61843c009b1
b9f5ec3d7b6085b5548b1

第8図



56b03813bad4c752a5c13247a0bc194ca607caf2e29564
6a061027d09c00d9ec9767f6e825c521647b16a19df9ee
6041ae400b7fa1026c93491d1d577a815129626493b6e9
da791e85203fd00018e6022a0215afb571b67fffd47d3e68
7dad79252ad98012bdd73d476edc0639a73cd9ca2a7f3c
831e065bdd

第9図


(a) 情報管理装置
START
S41
秘密鍵PR1を生成
S42
秘密鍵PR1から
公開鍵PU1を生成
S43
公開鍵を交換
秘密鍵PR1及び公開鍵PU2から
共通鍵CKを生成
S44
S45
セッション鍵SKを生成
S46
セッション鍵SKにより
一次変換データを暗号化して
二次変換データを生成
S47
セッション鍵SKを
共通鍵CKにより暗号化
S48
二次変換データに
暗号化したセッション鍵SKを
付加して送信
S49
二次変換データと
送信ログを保存
END
(b) 情報センタ装置
START
S51
秘密鍵PR2を生成
S52
秘密鍵PR2から
公開鍵PU2を生成
S53
公開鍵を交換
秘密鍵PR2及び公開鍵PU1から
共通鍵CKを生成
S54
S55
二次変換データと
暗号化された
セッション鍵SKを受信
S56
暗号化されたセッション鍵SKを
共通鍵CKにより復号
S57
暗号化された一次変換データを
セッション鍵SKにより復号
S58
復号した一次変換データを
データベースに格納
END

第10図

No.	氏名	生年月日	性別	医療機関名	傷病名	診療日数	診療内容
1	山田太郎	19700515	1	○○○	ーーー	ーーー	ーーー
2	小泉次郎	19551120	1	○○○	ーーー	ーーー	ーーー
3	日本花子	19990101	2	○○○	ーーー	ーーー	ーーー
4	山田太郎	19700515	1	△△△	ーーー	ーーー	ーーー
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

第11図

No.	ユニークコード	医療機関名	傷病名	診療日数	診療内容
1	548b1695d8e9a2b6085b5	○○○	ーーー	ーーー	ーーー
2	697473cd0029ca38c3	○○○	ーーー	ーーー	ーーー
3	4576edc003063c8381	○○○	ーーー	ーーー	ーーー
4	548b1695d8e9a2b6085b5	△△△	ーーー	ーーー	ーーー
⋮	⋮	⋮	⋮	⋮	⋮

1	548b1695d8e9a2b6085b5	○○○	ーーー	ーーー	ーーー
4	548b1695d8e9a2b6085b5	△△△	ーーー	ーーー	ーーー

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/03413

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/08, G09C1/00, G06F17/30, G06F17/60, G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/08, G09C1/00, G06F17/30, G06F17/60, G06F12/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	JP 2002-245164 A (Mitsubishi Electric Corp.), 30 August, 2002 (30.08.02), Full text (Family: none)	1,2 3,5-11,13 4,12
Y A	JP 2002-149497 A (NTT Advanced Technology Corp.), 24 May, 2002 (24.05.02), Full text (Family: none)	3,5-11,13 1,2,4,12
Y	JP 2002-279062 A (Toshiba Corp.), 27 September, 2002 (27.09.02), Fig. 9 (Family: none)	3,6,9,11

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 12 May, 2003 (12.05.03)	Date of mailing of the international search report 27 May, 2003 (27.05.03)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/03413

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-259219 A (Kabushiki Kaisha Kurei Fisshu), 13 September, 2002 (13.09.02), Full text (Family: none)	3,6,9,11
Y	JP 11-45304 A (Nippon Steel Corp.), 16 February, 1999 (16.02.99), Par. No. [0034] (Family: none)	5,6,13
A	JP 2002-109045 A (Medical Bank System Kabushiki Kaisha), 12 April, 2002 (12.04.02), Full text (Family: none)	1-13

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０３／０３４１３

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ９／０８，Ｇ０９Ｃ１／００，Ｇ０６Ｆ１７／３０，Ｇ０６Ｆ１７／６０，Ｇ０６Ｆ１２／１４

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ９／０８，Ｇ０９Ｃ１／００，Ｇ０６Ｆ１７／３０，Ｇ０６Ｆ１７／６０，Ｇ０６Ｆ１２／１４

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００３年
日本国登録実用新案公報	１９９４－２００３年
日本国実用新案登録公報	１９９６－２００３年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X Y A	ＪＰ ２００２－２４５１６４ Ａ（三菱電機株式会社） ２００２．０８．３０，全文（ファミリーなし）	1, 2 3, 5-11, 13 4, 12
Y A	ＪＰ ２００２－１４９４９７ Ａ （エヌ・ティ・ティ・アドバンステクノロジ株式会社） ２００２．０５．２４，全文（ファミリーなし）	3, 5-11, 13 1, 2, 4, 12

☒ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 １２．０５．０３	国際調査報告の発送日 27.05.03
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 石田 信行　5M　9469 電話番号　０３－３５８１－１１０１　内線　３５９８

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０３／０３４１３

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ ２００２－２７９０６２ Ａ（株式会社東芝） ２００２．０９．２７，第９図（ファミリーなし）	3, 6, 9, 11
Ｙ	ＪＰ ２００２－２５９２１９ Ａ（株式会社クレイフィッシュ） ２００２．０９．１３，全文（ファミリーなし）	3, 6, 9, 11
Ｙ	ＪＰ １１－４５３０４ Ａ（新日本製鐵株式会社） １９９９．０２．１６，〔００３４〕段落（ファミリーなし）	5, 6, 13
Ａ	ＪＰ ２００２－１０９０４５ Ａ （メディカルバンクシステム株式会社） ２００２．０４．１２，全文（ファミリーなし）	1 － 13